REMARKS

Applicants wish to thank the Examiner for the detailed and productive discussion of the application and its claims during the telephone interview on December 2, 2003.

This Response is responsive to the Final Office Action mailed September 15, 2003 in the above-identified patent application. The shortened statutory period for response ends on December 15, 2003. Accordingly, this Response is timely filed. The Commissioner is authorized to charge Deposit Account No. 50-0675 for any fee in connection with this Response.

Applicant respectfully requests reconsideration of the application. Claims 1-22 are currently pending in the application. Claims 1-22 stand rejected under § 103(a).

I. Obviousness rejection of Claims 1, 3, 5-6, 11, 13, 15, 17, 19, 21-22

Amended Claim 1 recites as follows:

> 1. A security system for a computer connected to a network of computers comprising:
> at least one security subsystem associated with said computer, said subsystem being configured to automatically and without human control correlate events across a plurality of devices associated with said network of computers and to detect attacks on said computer;
> and a secure link between said security subsystem and a master system enabling data communication therebetween; wherein
> said master system automatically and without human control monitors said security subsystem through said secure link and registers information pertaining to attacks detected by said security subsystem.

The rejection of claim 1 states that Messmer teaches that the black box located on the company network "is configured to correlate events across a plurality of devices associated with

the network of computers because Messmer teaches that a probe or "black box sensor" is put on the customer's network to accept audit data from a wide range of devices."

It has been known at the time of the invention that some smaller computer networks/systems currently generate, on average, 750,000 events per day. During peak times such systems may generate over 1,000,000 events in one hour. More intensive systems, however, generate approximately 3,000,000 events per hour, on average. Peaks of well over 20,000,000 events per hour are not uncommon for such heavier systems. Therefore, human analysis of this huge amount of events is not possible. Further, there was no adequate automated process in the prior art to automatically and without any human control to analyze and/or monitor this intense activity. As described in the amended specification, the subsystem and master system of the present Application are able to accept and correlate events from a plurality of devices without any human control. The system accomplishes this through software analysis of the events to determine the relevance of a particular event with regards to patterns of attack, historical trending, thresholds, anomalies, and other analytical methods. All of this analysis occurs simultaneously, and occurs at every level of the hierarchical architecture (or at a single node if there is no hierarchical deployment). The end result of this analysis is the discovery of an event (pre-attack activity, attack, or anomalous system activity) that will often require the involvement of an outside system or person to mitigate the risk of the attack, but that involvement is only required **after** the attack has been detected. Applicants amended independent claims of the present Application to more particularly recite the above discussed features of the invention.

Particularly, Claim 1 was amended to recite the limitation of "at least one security subsystem associated with said computer, said subsystem being configured to automatically and

without human control correlate events across a plurality of devices associated with said network of computers and to detect attacks on said computer," and the limitation of a master system which "automatically and without human control monitors said security subsystem." The element of automatically and without human control correlating events across a plurality of devices on the target network and detecting attacks on the computer is a part of the overall automated software-driven analysis performed by the entire system, and this particular part is performed by the security subsystem. Another part of this software-driven analysis is automatically and without human control performed by the master system.

II. Network Monitoring Performed by the "Black Box" of Messmer

As disclosed in the cited reference, the "black box" sensor "captures syslog and audit outputs" and "regularly transmits the network activity output in encrypted form to Counterpane's data centers ..., where it is monitored around the clock." (emphasis added). Therefore, according to the Messmer reference itself, the entire analysis of the captured and transmitted data is performed at the operating center by analysists, not by the black box. The black box only captures the security-related data and passes it onto the data center. Therefore, the black box does not automatically and without human control correlate events recorded in the syslog, audit outputs or in any other network activity output.

Additionally, Messmer teaches away from performing any part of the analysis without human control. It indicates that the analysis of attack footprints can only be performed by trained analysts located in Counterpane's data centers. Moreover, this language suggests that the analysis of attacks is not automated at all but rather fully accomplished by trained analysts.

Therefore, Messmer cannot meet a claim that recites "at least one security subsystem associated with said computer, said subsystem being configured to automatically and without human control correlate events across a plurality of devices associated with said network of computers," and a "master system automatically and without human control" monitoring the security subsystem. Thus, Claim 1 is patentably inventive over Messmer. Moreover, none of the other references cited by the Examiner disclose this limitation.

III. Other Rejected Claims

Similarly to Claim 1 above, independent Claims 8, 11, 13, 17, 21 and 22 all include the limitation of performing the event analysis, i.e., " correlating events across a plurality of devices," and "monitoring the status" of the detection means, automatically and without human control. Therefore, Claims 8, 11, 13, 17, 21 and 22 are patentably inventive over Messmer. Applicants respectfully submit that dependent Claims 2-7, 9, 10, 12, 14-16, and 18-20 are likewise believed to define patentable subject matter in view of their dependency upon allowable independent Claims and, further, on their own merits.

IV. Obviousness rejection of Claims 2, 8, 12, 16 and 20

Claims 2, 8, 12, 16 and 20 have been rejected by the Examiner as unpatentable over Messmer and Newton's Telecom Dictionary, in view of Kurtzberg et al.

Applicants reiterate all arguments presented above with respect to Claim 1 because Claims 2, 8, 12, 16 and 20 all include the limitation of automatically and without human control correlating events across a plurality of devices and monitoring the status of the detection means either in their own text or in the text of their base claim. As discussed above, Messmer cannot

meet a claim that recites such limitation. Therefore, Claims 2, 8, 12, 16 and 20 are patentably inventive over Messmer.

Moreover, none of the other references cited by the Examiner disclose this limitation.

V. Conclusion

In view of these remarks, Applicant respectfully submits that the claims are in condition for allowance. Applicant requests that the application be passed to issue in due course. The Examiner is urged to telephone Applicant's undersigned counsel at the number noted below if it will advance the prosecution of this application, or with any suggestion to resolve any condition that would impede allowance. In the event that any extension of time is required, Applicant petitions for that extension of time required to make this response timely. Kindly charge any additional fee, or credit any surplus, to Deposit Account No. 50-0675.

Respectfully submitted,

Schulte Roth & Zabel LLP
Attorneys for Applicant
919 Third Avenue
New York, NY 10022
212-756-2000

By: Anna Vishev
Anna Vishev
Reg. No. 45,018

Dated: December 15, 2003